Customer Awareness - Cyber Threats and Frauds

Fraudulent phone calls and SMSs containing fraudulent URLs on the subject of KYC updation, linking of bank accounts, seeking confidential information of customers, are currently in circulation.

Fraudsters attempt to get confidential details like user id, login / transaction password, OTP, debit / credit card details such as PIN, CVV, expiry date and other personal information. Therefore, keep yourself safe from Banking frauds and learn he tricks to avoid cyber frauds.

RBI urges the members of public to practice safe digital banking wile carrying out digital banking/payment transactions.

Safe Digital Banking Practices

1. Never share your account details such as account number, login ID, password, PIN, UPI-PIN, OTP, ATM / Debit card / credit card details with anyone, not even with bank officials, however genuine they might sound.
2. Any phone call / email threatening the blocking of your account on the pretext of non-updation of KYC and suggestion to click link for updating the same is a common modus operandi of fraudsters. Do not respond to offers for getting KYC updated / expedited. Always access the official website of your bank or contact the branch.
3. Transactions involving receipt of money do not require scanning barcodes / QR codes or entering MPIN. Thus, exercise caution if asked to do so.
4. If you receive an OTP for debiting your account for a transaction not initiated by you, inform your bank immediately. If you receive a debit SMS for a transaction not done, inform your bank immediately and block all modes of debit, including UPI. If you suspect any fraudulent activity in your account, check for any addition to the beneficiary list enabled for internet / mobile banking.
5. Regularly check your email and phone messages for alerts from your financial service provider. Report any un-authorized transaction observed to your bank immediately for blocking the card / account, so as to prevent any further losses.
6. Secure your cards and set daily limit for transactions. You may also set limits and activate / deactivate for domestic / international use. This can limit loss due to fraud.
7. Never continue default passwords for any electronic devices/connections/Applications/Apps
8. Never store the passwords in the system or allow the system to remember
9. Never share Your or Bank's passwords with anybody else. Banks never ask for your passwords
10. Never Click on Links sent through Email / SMS
11. Do not respond to Email/SMS where the Sender doesn't address you by name.
12. Never click/use unknown websites offering freebies/Discounts
13. Verify the https:// and correct name of the organization in the address i.e. URL
14. Verify the Lock symbol in the URL before you give any information
15. Never open mails from unknown sources
16. While making online transactions with credit/debit card, user must use his/her card only at established and reputed sites as there are less chances of card fraud on a reliable website.
17. Always ensure that the address of the website, where transactions are to be done, starts with "https://" and not "http://".
18. Change your card PIN (Personal Identification Number) periodically.
19. Do not disclose any personal information online like your date of birth, billing address, etc., on the Internet because that can be misused in order to unlock your account password.
20. Avoid sending card and account details through e-mail to prevent from malicious use by others.
21. Report any loss due to cyber frauds to the Number 1930 or contact corporate office Phone number 040-41923047 mail ID info@kbsbnkindia.com.